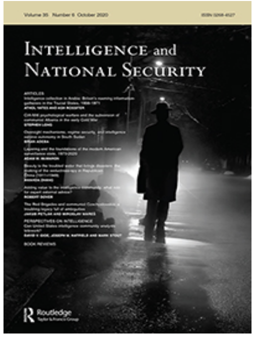

Routledge
Taylor & Francis Group

Intelligence and National Security

ISSN: (Print) (Online) Journal homepage: www.tandfonline.com/journals/fint20

Adding value to the intelligence community: what role for expert external advice?

Robert Dover

To cite this article: Robert Dover (2020) Adding value to the intelligence community: what role for expert external advice?, Intelligence and National Security, 35:6, 852-869, DOI: 10.1080/02684527.2020.1793060

To link to this article: https://doi.org/10.1080/02684527.2020.1793060

Published online: 13 Jul 2020.

INTELLIGENCE AND NATIONAL SECURITY
2020, VOL. 35, NO. 6, 852–869
https://doi.org/10.1080/02684527.2020.1793060

Routledge
Taylor & Francis Group

ARTICLE

Adding value to the intelligence community: what role for expert external advice?

Robert Dover

ABSTRACT
Reviews of intelligence failures have recommended greater use of external expertise in challenging intelligence community assessments. External contributions were expected to augment covert collection and to provide open-source challenge to analysts, rather than to directly contribute to decision support. The structural limitations of the scope and machinery of intelligence have limited the value agencies can extract from external experts. Creating an Open-Source Intelligence Agency of commensurate size to primary intelligence organisations would enable decision support to be provided to all government departments. It would widen the pool of sources and experts, providing for greater extraction of value from experts who are only partially included in this government activity.

After the 2003 Iraq war inquiries on both sides of the Atlantic recommended that intelligence services make more use of external expertise, including that provided by academics. External contributions were expected to augment covert collection and to provide open-source challenge to analysts, rather than to directly contribute to decision support. The two structural limitations of intelligence to (1) a narrowed scope of securitised issues and (2) the organisation and processes surrounding engagement have constrained the value intelligence agencies can extract from external experts. Whilst the examples drawn upon here and the assessment applies mostly to the United Kingdom, there are clear resonances to the intelligence community in the United States, where open-source intelligence enjoys a better developed and discrete institutional backdrop via the CIA's Open-Source Enterprise within the Directorate of Digital Innovation, and within the all source fusion of the Joint Intelligence Operations Center Europe (JIOCEUR) Analytic Center (JAC – based in the UK),[1] but where the same underpinning tensions exist. Creating an Open-Source Intelligence Agency of commensurate size to the existing primary intelligence organisations would enable intelligence to provide decision support to all government departments. It would also widen the pool of sources and external experts in the intelligence community, providing for a far greater extraction of value from experts who are only partially included in this government activity. Within the current system of engaging external experts, there is a form of unionisation around certified expertise, and a barrier to multi-lingual and multi-locational knowledge as part of the intelligence knowledge pool. This article argues that there is scope for improving the engagement of external experts within the existing machinery and mechanisms, but only a paradigm shift to an open-source platform geared to providing decision support to government departments and elected officials will yield dramatic improvements.

The contemporary security threats require intelligence officers and their employing agencies to work to increasingly tight schedules, across contested datasets and models against adversaries enhanced by the tools of globalisation.[2] This is as true for biosecurity threats such as COVID-19, as it does for Russian, Chinese, Iranian and Jihadist positioning and aggression, and the disruption caused by organised crime gangs.[3] The post-9/11 Jihadist threat came to be typified by the term

CONTACT Robert Dover rob.dover@leicester.ac.uk

'glocal' – the global and the local – and this gave rise to misleading accounts that this phenomenon was both new and novel.[4] In reality, modern forms of globalised travel, finance, communication and manufacturing had merely accelerated this historical trend, but few in western governments tracked this trend because they were understandably focused on operational necessities. Furthermore, and for much of modern human history globalisation had favoured the global north, but through the rise of jihadist terrorism and the growth of Chinese economic strength and hard- and soft-power tools, it is possible to convincingly argue that neoliberal globalisation has been turned against the global north.[5] Similarly – with the case of COVID-19 – the increased interdependency between north and south has seen a pathogen originate in the developing world and decimate the economies of the global north, prompting some observers to ask 'has China won'?[6] In the face of these 'wicked' problems,[7] by which I mean public policy challenges with substantial complexity, it is easy to make the case for a widening of the pool of external experts to assist governments and their intelligence gathering organisations to conceptualise and mitigate these threats.[8]

The challenge of COVID-19 has led western governments to make calls for whole national efforts, evoking wartime sentiment and mythology.[9] In the UK this has included ambitious calls by Parliament and the Cabinet Office for academics and industry experts to register their expertise to assist in the government's response.[10] This process called for particular kinds of certified expertise. Similarly, the research funding agencies placing financial resource at the disposal of academics and those working in small and medium enterprises to bid in to complete rapid response research programmes to improve our understanding of all aspects of the pandemic and its impact on society and government.[11] The governmental response to COVID-19 echoes some of the conclusions of the 2012 *Blackett Review* which highlighted the benefits that could be accrued from drawing upon external expertise such as: to inform key risk assumptions; to inform judgements and analysis; to better detect early signs of strategic shock or surprise; to inform the development of internal and external risk communication strategies; and to strengthen the scrutiny of the National Risk Assessment.[12] Although these recommendations were identified in the context of specific types of risk assessment, the recommendations are widely applicable to other areas of assessment and analysis across the UK Government, albeit not concerning pandemics where government preparedness was rolled back to allow officials to spend a greater amount of time in 2019 preparing for *Brexit*.[13] In the context of a preponderance of 'wicked problems', the key question of this article seeks to answer is: what do we need to change about our intelligence and assessment model and processes so that we can harness experts across disciplines and languages to become essential in the decision support function to government across all public policy areas?

To answer this research question, this article is structured to provide a critical commentary on the existing patterns of external engagement in intelligence work. The article moves onto provide an assessment of the barriers present to the effective incorporation and engagement of external expertise into the intelligence community, followed by an evaluation of where opportunities exist within the existing model of engagement. The article then identifies where opportunities sit within a competing open-source model that has a stronger focus on a wider model of decision support to government and elected officials. This essay is premised upon sources from the extant literature, triangulated with participant observations I have made as an academic granted the opportunity of seeing three analytical communities at close quarters during a period stretching from 2016 to the COVID-19 lockdown in 2020, funded by the Economic and Social Research Council (ESRC) Impact Accelerator.[14] It is contractually impossible to bring forward precise examples from these settings into the article, without breaching rules around discretion and confidentiality. What I am able to do, however, is to provide my participant observations as an artefact capable of being critiqued by others, supported by independent evidence and research in the extant literature.

The uneven case for external expertise to be incorporated in intelligence

Phillip Davies, speaking at the 2004 Political Studies Association conference engagingly captured the possible reasons for intelligence failure in the case of Iraq as: 'asking bad questions', 'to poor collection', 'to poor assessment' or 'to poor usage, in other words, the problem of bad politicians'.[15] If we follow Davies' logic on, and insert the question of what an external expert might provide to the production of intelligence assessment, we are forced to ask the a priori question of what we mean by the term 'expert'? Is an expert someone with experience or proximity to an issue? Is an expert someone with a publication record on a subject? It is interesting to note that the UK government's call for experts in March 2020 asked applicants if they have published on COVID-19 which, given the World Health Organisation (WHO) had yet to deem it a pandemic somewhat misunderstood the nature of academic publishing.[16] Is an expert someone with higher-level degrees in relevant subject areas? Can an expert be someone without higher-level degrees, but with years of onsite experience in a relevant industry? We know that the notion of expertise has become subject to public contestation over the last decade. The British government Cabinet Minister Michael Gove's infamous rejection of experts became a shorthand for an era of political discourse in which having online traction became more important than substantive expertise on a subject.[17] In an intelligence setting an external expert should be defined in terms of: *(expert = subject knowledge + experience + motivation).* The latter element has a particular resonance in intelligence (and perhaps belies the notion that external experts are a form of human intelligence) because the motivation of human sources is an important determinant in judging the reliability of their advice or assessments.[18]

The answer to the question of 'what is expertise?' also turns on whether a holistic or narrow analytical model is being utilised. From my experience as an academic who has been allowed to carry out extensive periods of observation within several analytical communities, I note later in this piece that government intelligence (both in national and sub-national organisations) largely locates itself narrowly around militarised security or quasi-militarised issues. Thus, most analysts are focused on the lethality of the threat: that leads them into equations around capability and intentions. Law enforcement intelligence analysts focus on the magnitude of the harm and the sentencing structure of the offence.[19] This is also a version of capability and intentions, albeit one that also contains a far larger component of tactical intelligence.[20] Holistic analytical models are premised upon the breadth of the problem, challenge or issue. These models are premised upon a reality that open-source collection will generate peaks of interest where covert collection can then be targeted. Holistic models are founded upon a greater weight of open-source materials, which does not include communications intelligence intercepts (per *Operation Rubicon* or the Edward Snowden revelations) and on a plurality of analytical methods and processing techniques.[21] Because these models are premised upon information sciences and human intelligence, they are far closer to these disciplines key concerns of information surety, geo-tagging and so on.[22] It is possible to argue that the warehousing and large n-analysis of, for example, mobile phone meta-data, CCTV or dashcam footage, or online shopping activity are both valid and useful in a holistic analytical model, even one premised mostly around questions of lethality. The issues of trust and transparency are particularly acute around these forms of data, even if crowdsourced solutions (such as *Waze* for traffic movements, or *Air-Quality.com* for pollutants and allergens) have been shown to be effective, albeit in consumer information applications.

For some questions, the notion of who can be considered an expert can be reasonably bounded by technical qualification and experience. In the COVID-19 pandemic qualified and experienced virologists and epidemiologists have the greatest chance of generating research questions and then the research designs to produce the most useful and usable types of data for public health responses, even if some of their projections have been heavily criticised.[23] But where behavioural psychologists have been used to translate public health response into public policy the connection between expertise and outcomes has looked more tenuous.[24] In the UK, the behavioural scientist groups advising the government placed a great deal of weight on the British people only being able to sustain a lockdown when the infection and death rates had reached a substantial level.[25] The response from the British public was to effectively lock-down prior to the government's instructions. In this instance, bartenders, retail workers and street sweepers would have been better placed, or more expert, in reading the public's sentiment than the qualified experts. So, whilst the further, higher and continuing professional development industries award qualifications via established processes of learning and participation, we can observe that certified expertise was notably weak in predicting and responding to the development and growth of jihadism, the 2008 financial crisis and the 2020 COVID epidemic, three of the four significant challenges of the modern era, the last being climate change, where the failures have been mostly political.[26]

In the context of the weakness in certified expertise advising government, it is easy to see, as noted earlier, how prominent politicians advocated for the rejection of certified expertise, something that strongly resonated with the public.[27] For an intelligence community looking for insights to provide competitive advantage, it is as necessary to recruit certified expertise from established and quality education providers, as it is to look into less obvious pools of expertise – be it within hacker communities, on the ground in emergency rooms within hospitals, spotters, those with a deep knowledge of money movements, or those close to illicit organisations, for 'real' or authentic expertise.[28] An early modern proponent of open-source intelligence, Robert Steele, was undoubtedly correct to suggest that OSINT is an 'intelligence multiplier' if used and targeted into the analytical machine correctly.[29] Jennifer Sims argued that OSINT could convey 'decision advantage' to officials, which is retained within my preferred term 'decision support'.[30]

The currency of degree qualifications in intelligence (and outside) has come under pressure as employers ponder the disconnect between candidates' educational experiences and their real-world requirements: does a degree in criminology equip a student with an ability or insight into how to manage covert human sources, does a degree in economics provide adequate insights into combatting money laundering? Such questions have – in the UK – seen a resurgence of apprenticeships, albeit within the historically unusual setting of higher education degrees. In the intelligence community, there has been an acknowledgement of intelligence as a vocation through the national occupational standards (currently being replaced by a Skills Framework and the apprenticeship standards) and via the new programmes of intelligence education provided through the Cabinet Office.[31] These new forms of training combine education with on-the-job training: a compelling form of blended learning that relies on protected time and teaching staff with the right combination of experience and intellectual calibre. In the US there is a far greater emphasis upon professional intelligence education and training, which is delivered within the agencies, within university partners and via the National Intelligence University in Washington. So, whilst there is a clear drive towards a form of university certified vocational qualification, there is similarly a continued operational requirement to continue exploring parallel forms of expertise from those engaged in relevant occupations or activities.

The notion of external expert engagement is underexplored in the extant literature, but also in practitioner circles. From an academic perspective Michael Goodman, Martha White and I (in various combinations) have made what we suggest is the practitioner case for enhanced engagement as providing enhanced coverage in: 'Trends analysis based on statistical data capture … Corroboration or validation from academic research that has undergone more rigorous testing and research techniques … Corroboration or validation from academic research conducted at a more granular level in terms of topic matter. Corroboration or validation analysis from academic research derived from a wider or alternative pool of information'.[32] It could also be noted that academics provide a longer-term contextual perspective, that might be alien to government analysts due to their time pressures and short-term focus. In the context of the Iraq and Afghan campaigns, we might reflect that academics with area studies and theological expertise would be particularly valuable.

From activist and independent journalist websites – which often produce interesting and valuable material – the question of what engagement is mis-specified or under-defined. An individual attending a Whitehall event will often be described as an insider. Academics providing evidence to Parliament, with a line of argument that activists find troubling, will again be described as government insiders, doing the government's bidding or in pejorative terms – as I have been – as a 'government shill'. Here the texture of the debate is troublingly close to Cold War taxonomies around 'useful idiots' and 'fellow travellers': the released Cold War archives of the Eastern bloc tell us that the size of Soviet agent rings in the west was dependent upon the exaggerated reporting of Czech and East German intelligence officers, in particular.[33] This pattern of labelling is also close Michael Herman's less charged evocation of the Tudor term 'intelligencers', which is a hierarchical taxonomy of agents from those actively recruited down to those returning from foreign travel consulted about their views, who are oblivious to the purpose of the questioner.[34]

From my research observations within three analytical communities, the UK and US national security communities could straightforwardly increase its contacts across a wide range of disciplines, research organisations, universities and think tanks domestically and internationally, within its existing model of engagement. In doing so, these communities could leverage or influence the direction of these external researchers through meaningful medium-term reciprocity rather than going through the more difficult process of identifying proper research funding. Access to the views of the national security community on mutual topics of interest, and the chance to use academic research to inform and impact upon decision-making on issues of national security, is likely to be incentive enough for those external experts who are already predisposed towards the public service element of engaging with practitioners and have the motivation to do so.

If the relationships are organised well, the benefit of practitioner-external expert engagements should not just fall on the side of the national security community. There is potential for external practice communities and individual experts to also benefit through a closer interaction between these two worlds, but there is little evidence for this benefit at the time of writing. Indeed, my own professional experience suggests that the expectations of practitioners are that this engagement is something that external experts should *want* to do for the government as an end in and of itself, and further should be willing to do so to the partial detriment of other professional duties. This is not as unreasonable a position as it might seem at first glance. Motivation has always been an important factor for intelligence officers measuring the potential reliability of human sources, and my sense is that the attitude towards external experts fits on this spectrum for security officials.[35]

Within the existing model of engagement, the main benefit for the security community is *corroboration and challenge analysis*, and the same applies for the individual external experts. Engaging with intelligence officers or analysts who are analysing similar topics using classified data has the benefit of providing them with informal measures of quality control, corroboration or confirmation to hypotheses and judgements, providing the officer feels so moved to express a helpful opinion. An external review function from a practising analyst can be very helpful to externals, helping them avoid erroneous conclusions and maintaining their reputation in the practitioner field, opening up a hard-to-reach form of peer review. The benefits to external experts, within the existing model, are heavily contingent on the ability and willingness of a closed analytical community to communicate their views in confidence or at an unclassified and non-compromising level. Such willingness is very closely aligned with issues of trust. This will be dependent on the internal risk versus benefit assessment of the closed analytical community and places the external in a supplicant position as regards knowing or understanding the quality of information they are receiving. It is the wrapper of secrecy that degrades some of the value in the exchange. Some, like Bowman Miller argues that agencies need to protect even the OSINT they generate to avoid gifting usable material to rival agencies, and he points to Chinese publishing practices to reinforce this point.[36] My point is that the compulsion to secrecy in this area changes the relationship between producers and consumers, and conditions the knowledge being produced. The problems around the authenticity of knowledge exchange are largely removed within an Open-Source Intelligence Agency, because the Agency is a producer in its own right and is producing content on public policy areas agnostic to input constraints, in other words, the need for covert collection or requirements.

Greater levels of embedded engagement within existing models – through a form of Reservist programme (in the UK, the nearest equivalent is the National Crime Agency's Special Officer programme) or working as a contractor – are a good opportunity for the agency to exploit external expertise and gain targeted insights on classified materials. Similarly, these insider engagements provide a good opportunity for the external expert to experience practitioner life on the inside, rather a curated or carefully guarded snapshot of that life provided by workshops or interviews and the like. But embedded relationships – within the existing model of engagement – require an agency to sponsor the external's security clearances incurring a financial cost and a cost to officer time, it requires the agency to manage the volunteer, to provide them with physical passes, internal-electronic passes and if they are to gain access to the intranet, or equivalent, a laptop and telephone, as appropriate.[37] Such a level of expenditure requires the hosting agency to put forward what they describe as a business case to justify the cost against the anticipated gain.

For the external expert, they have to be intellectually and politically sold on the idea that this wish to assist the government's security effort that they have the time and willingness to compromise their other professional commitments and be willing to put themselves forward for the level of personal intrusion that a security clearance process entails.[38] These willing volunteers also have to be willing to accept the obligation that official secrecy and the surrounding processes entail and they have to accept a partial curtailment of their normal freedoms to publish, if that applies to their external existence. The pervasiveness of web-crawling technologies means that once information is released it is practically impossible to 'un-release'.[39]

So, we have to build into our understanding (and the gap between perception and reality) of the role of expertise in the intelligence community that engagement has been poorly defined and that many of the people who are being sought or who engage with the community do not know they are doing so. There will be a sliding scale from those who are overtly recruited and security cleared, down to those who are met by chance or confected chance. This sort of engagement is – therefore – a form of human intelligence activity. As such we should also note that one of the reasons for the intelligence community to embrace external engagement is that will provide them with greater access to a wider pool of covert sources and links brokered by trusted intermediaries. Cynically, there are more opportunities to do this with the creation of an appropriately sized Open-Source Intelligence Agency than under the existing arrangements.

For the readers of this journal, it will be well known that it is impossible to do intelligence effectively without a solid platform of open-source intelligence to provide context. We should also note that, for officers, it is impossible to know whether their intelligence work has been effective without fully functioning counterintelligence capability. This is something that the Five Eyes group has let slip since the end of the Cold War against Chinese and Russian adversaries in particular. But rather than pouring in greater resource and effort within the existing intelligence model, it would be more effective to change the model and then more tightly confine counterintelligence work to the then limited range of activities it would then apply to.

The barriers before the experts

Having struggled to find appropriate mechanisms to bring in external experts, intelligence communities have then often failed to utilise this expertise they have engaged with. Having been given permission to closely observe some of the work of the UK's Cabinet Office, the UK's National Crime Agency and an intelligence branch of NATO, I have observed the following self-sustaining logics that creates operational barriers and underpins this underutilisation.

The secrecy imperative

The mantra of 'without secrecy, it isn't intelligence', may seem somewhat blunt in the twenty-first century, but we can observe that the concept of secrecy structures, shapes and conditions the intelligence community. The culture around the intelligence community is – for all good reasons – founded upon secrecy, confidentiality and discretion.[40] All government intelligence officers are subjected to the vetting or clearance process prior to being admitted into the community. The application process relies upon the individual officer maintaining discretion and thus not disclosing their application to friends and family, whilst basic training is heavily conditioned by a trainee's ability to maintain discretion and to understand advanced techniques in achieving this. Consequently, it should be little surprise that the intelligence community maintains careful rules of engagement for outside experts and a variety of more or less intrusive protocols for those doing so, around disclosure and debriefing. For example, in the UK intelligence community, I was told that discussions with a journalist or investigator would necessarily lead to a disclosure report having to be filed and on occasion a debriefing process to occur. It would be reasonable to assume that there would be disciplinary (and vetting) consequences for any officer not following these protocols. Similarly, in the US intelligence community, contemporary history relates that discussions with journalists could be authorised, but would be subject to extensive debriefing, and career consequences if not followed.[41] Gibson noted that this mismatch of cultures often led to a misperception of OSINT being in competition with closed-source intelligence.[42] This is a cultural barrier – around secrecy – that needs to be overcome.

For external experts, the current 'challenge' function they sit within creates additional problems to noting the impact they have made on the intelligence community: something that might be useful to them for career or commercial reasons. If they are not able to note it – and it is reasonable to expect that they are not – then what incentive does the external expert or their employer have for allowing their member of staff to engage on these issues? These seem external experts cannot unknow what they have learned, however, just not to repeat it in unauthorised settings. Such challenges are less problematic within an Open-Source Intelligence Agency, where any direct intelligence requirements can be straightforwardly managed, and where the core business is the production of verified baseline information and assessments across the broad sweep of government activities.

Whilst open-source intelligence is a large component of the 'all source mix', covertly collected intelligence tends to be described in terms of it being of higher value to analysts.[43] This may be a matter of human psychology that the harder to achieve artefact is, therefore, more valuable. We see soft evidence of this in political memoirs and the primacy afforded to secret documents and secret information. It is also the case that militarised forms of security lend themselves far more straightforwardly to covert collection, although not exclusively so, than intelligence and actionable information around pandemics, climate change or patterns of economic dislocation, but which remain relevant to decision support for public policymaking and strategic intelligence.[44]

When it comes to international experts, the issues around counterintelligence once again come to the fore. The vulnerability of a foreign power having a close knowledge of what the intelligence community is interested in, the questions they are asking, and what information was shared is a significant disincentive for this form of engagement, even though the added value such sources would be able to bring are considerable, particularly if an agency is looking to tackle a transnational (or *glocal*) threat. The challenges of radicalisation and of international terrorism are the most obvious of a suite of challenges that suits a broader consultation of multinational and multilingual sources and experts.

The structure, disposition and funding of intelligence

The business of intelligence and of intelligence assessments has been influenced and shaped by some of the logics of neoliberalism. The use of key performance indicators (KPIs), of editorial processes that emphasise rapidity and customer satisfaction, and of an incentive structure that – in effect – filters from the lower grades to the top, has placed this most public sector of business areas into the realm and logic of management sciences. Within a system that is analogously similar to just-in-time and just enough processes that we can observe throughout the economies of the global north of the emphasis is – more often than not – to fall back on tried and tested sources, methods and open-source outlets and techniques. There is rarely the time built into any realm of national security, law enforcement, or even strategic intelligence service for ‘soak time’, to build up a wider context, or to consult unusual or untested sources that might provide interesting or unique angles on a problem. Instead the requirement is for ‘the answer’, or deployment of Person X who is known to have some expertise in the area that is of interest.

Government intelligence analysis, as a knowledge production process, is concerned with distilling empirical truths and positioning policy or government assets in response to the particular issue or threat. It is not a foundational science and therefore does not seek to posit fundamental truths in an environment that exists outside of the context in which it is made. Thus, the facets that I have observed as being vulnerabilities or weaknesses might be nothing of the sort (from a government perspective) as the existing processes are widely seen within the policy community as being sufficient for the task. Is there genuinely the appetite within senior public policy circles for uncomfortable or paradigm breaking truths?

The connection between civilian or wider-world ideologies and practices has served to create intelligence cultures where the acquisition of wider pools of expertise is rendered problematic by the under-resourcing of analytical pools, the time demands on assessment staff, the formulaic ways in which assessments are presented and delivered and the rigidity of security considerations that close off the vast majority of external expertise to the community. The rationale for these choices has been framed in terms of the security state being subject to the same value for money pressures as the rest of government. The requirement to provide evidence of value for money relies upon there being measurable indicators of productivity and impact against agreed benchmarks. So, neither an individual analyst nor their line managers can afford to be seen as unproductive, according to the number of assessments produced, or to produce time-consuming or lengthy assessments on static issues, because that does not represent value for money. But such pressures result in cookie-cutter assessments: the same range of sources, using the same techniques and presentations. The history of the AQ Khan saga tells us that in using the same analytical lenses that analysts – even with sufficient raw intelligence to understand that the AQ Khan programme was substantial and enduring – concluded that no sub-state actor could be capable of mounting a nuclear weapons programme.[45] Similarly, the fall of the Shah of Persia in Iran is described as a strategic shock, an intelligence surprise, when Robert Jervis’ research tells us that cognitive dissonance accounted for the failure to understand what was developing in Iran.[46] The Operation Rubicon papers – revealed in 2020 – compound this yet further, as they show that the US Administration had communications intelligence that showed precisely what was developing in Iran in 1979, but this did not shift the intelligence assessment.[47]

These examples provide some evidence that there is a utility in allowing for parallel analytical processes that might result in failure or null hypotheses. Would an unvettable, outsider area studies specialist in 1978 have been able to point to unfurling developments in Iran that gave the US and UK early warning of regime change? We need only dip into the archives around the approach to the Iraq conflict to see this similar pool of area studies specialists warning of insurgency and enduring civil conflict in the event of war, not from overt or campaigning political positions, but from an assessment of the societal contours in the Middle East.[48] From the evidence provided to the Chilcot Inquiry, there were a small number of voices suggesting this but no systematic means for these assessments to gain traction.[49] The British Prime Minister’s key advisor, Dominic Cummings, asked in December 2019 for ‘misfits and weirdos’ to apply to work in the Cabinet Office, on public policy and forecasting.[50] Cummings’ support for systems thinking, of identifying trends that emerge from a system, a branch of thinking that has some of its origins in ecological studies, and of viewing politics as a form of ecology, is a significant area that is underexplored in intelligence analysis.[51] Such an approach does produce paradigm shifts; indeed, from a systems perspective, it is possible to see the US as an adversary competitor to the UK, rather than simply a competitor and ally. These sorts of conclusions are clearly uncomfortable in the policy realm because they unseat long-held views and preferences. Whether it is desirable to include them in the policy mix rather depends on whether one believes intelligence is around speaking truth to power (an outsider role), or providing ‘best truths’, within an established set of processes and norms (an insider role). The former involves widening the pool of contributors – which tends to be equated with additional expense – but which helps to facilitate multiple lines of assessment (some which fail), allowing for longer term and slower forms of analysis, things which can be interpreted as being economically inefficient.

The security imperative demands that external experts brought into provide answers to official questions, as part of an intelligence requirement, should be eligible for or have received security clearances. This is not always the case, as there are ways in which uncleared experts can be consulted in unsecured environments, and asked a multitude of questions only one or several of which will be 'the real ask', or they might be asked questions in a plausibly deniable setting, such as at a conference or workshop by a undisclosed individual. The amount of value to be accrued through these indirect approaches is open to question, particularly as they do not open much in the way of opportunity for follow-up or deeper questioning. The more direct approach, of bringing external experts inside the security tent is variously and paradoxically considered to be the cheap option, the prohibitively expensive option or the too-complex-to-manage option. Providing that security clearances can be transferred from one agency to another, which is not always guaranteed because of the vagaries of who owns the registration, who sponsors and has paid for the clearance and so on, this represents the simplest option for an agency wishing to bring in an external expert. In effect, the subsequent agencies are free-riding on the originating agency's sponsorship of the external. One of the consequences of this pattern of behaviour is that a cleared expert might be asked to provide advice and support to multiple agencies: they become, in effect, the first port of call, because the transaction costs of engaging them are proportionately smaller than if they were engaged from fresh.

The costs associated with engaging an external expert are contested. Where costs are publicly available, and in the UK, the basic level of vetting – Security Clearance – costs just under £200 (per the UK College of Policing's website, but it is not clear if this is a subsidised rate). According to American open sources, the equivalent cost is circa 450. USD Others cite the cost of the Security Clearance between two and five thousand pounds and the far higher Developed Vetting (DV) as being between ten and twenty thousand pounds to process. Again, in the US open sources put this figure in the US at circa 6000. USD There are no open-source valuations for the UK DV process, so it is difficult to know, but it seems beyond the reach of most private individuals when it is not accompanied by additional earning potential, or external funding covering the costs. The real cost to the agencies is in the counterintelligence and security function. Externals who are within the security wrapper of an agency will have multiple professional personas, and therefore a work obligation to another, paying organisation (creating its own security challenge), external work IT and email addresses, devices and so on. The complexity of managing the security of those paid employees of an agency is significant, but the complexity is exponential for those externals who are – in effect – insider-outsiders. There are significant reputational risks to agencies from the behaviour or professional conduct of externals, and similarly, additional risks incurred by externals often for no financial reward. These insider-outsiders can often roam relatively free (outside of indoctrinated operations) within agencies assisted by many staff being unsure (and perhaps afraid to ask what the limits of their status is) and thus assisting across a wide array of issues and policy areas. According to those who have left the CIA, the agency forbids its clandestine staff direct contact with subject matter experts, instead preferring to route them through the agency's Open-Source Center.[52] The employment of externals is, therefore, one that places a considerable management burden on recipient agencies, and a business case to justify the additional imposition upon staff.

A key barrier to the incorporation of external expertise into the intelligence process is throttled access to key groups, such as academia, civil society including religious and labour organisations, businesses, local government, both legacy and new media, the armed forces including reservists and the not-for-profit sector – that possess direct access or hands-on knowledge – capable of providing or generating knowledge that is useful to the intelligence community.[53] These groups are not well suited to being managed by clandestine case officers but would indeed be more effectively managed by overt or open case officers. Both sides of the Atlantic intelligence agencies have been noted as being adept at debriefing legal travellers, but others have argued that these activities have morphed into fronts for entrapment and trafficking of various kinds.[54] Whilst the history of modern intelligence suggests that agencies from all countries have often balanced ethical probity with operational necessity, there are opportunities being missed if these forms of overt approach have been dialled down whilst more coercive forms have been dialled up. If intelligence really reflects the society it serves, then it is one that is more cynical than is commonly accounted for in the literature.

This vulnerability in collection also suggests opportunities for reform in the management of HUMINT. The increasing emphasis on signals, electronic and communications intelligence, in part due to the perceived certainties of these forms of mass and/or covert collections and in part because of the length of time to cultivate human sources, the risk of doing so for the target, for public relations and the financial implications for uncertain ends, has diminished the role of HUMINT. But HUMINT that accesses the full breadth of knowledge-producing groups, in both overt and covert ways should be capable of adding considerable value to the intelligence products. Similarly, and starkly demonstrated by the failure in the UK to address adversary intelligence agencies operating aggressively, that counterintelligence has been under-funded and under-developed and when it comes to Russian intelligence activity, seems to have been merely going through the motions rather than offering a serious opposition to adversary activities.

The problem of sourcing: utilising multilingual sources

OSINT has been incorrectly conflated with making greater or better use of online searches, whilst failing to acknowledge that consumer online searching (via Google and the like) is problematic because these services are only indexing an estimated 3% of internet material, and thus leaving the vast majority of online material unindexed.[55] Of that collected in the US by the National Security Agency (NSA), only 1% is said to have been analysed, let alone proven to be useful.[56] So, there needs to be some work done to improve the public understanding of what OSINT actually involves, and a democratisation of advanced internet discovery tools to provide more open access to the full range of information being provided in publicly accessible locations. The unindexed web (publicly known as the Dark Net or Dark Web) has become synonymous with criminality, abuse and whistleblowing, and it requires some specialist knowledge to navigate it, giving it the feel of 'the other'. Whilst there are specialist internet investigation tools used by government analysts, including those used to examine individuals, sentiment and trends, they are labour intensive (in the training, and usage) even whilst saving a considerable amount of officer time. What has not been achieved is the successful development of a back-office function that systematically processes this material for analysts, and one which could be used across the whole of government as a form of open-source decision support function.

Analysts are challenged when constructing context and sense from open sources. They face constraints in accessing the broad sweep of published academic and technical sources from behind publisher paywalls, which is a surprisingly common and large constraint even within affluent intelligence systems. Analysts tend – very reasonably – to lack the advanced critical and socialised skills to understand the merit of a particular publication, what the outlet is known for and how it came to publish the respective piece, and – much like the rest of those employed in post-industrial societies – the necessary time to read these sources properly. Linked to this neuroplasticity is beginning to impact upon analytical craft: analysts are similarly used to reading on screens, of skimming, surfing, filtering and consuming ever shorter forms of information.[57] Spending prolonged periods of time-consuming these truncated forms of information has been shown to reduce the attention span of high-volume readers, and assists in generating confirmation biases. This problem has been recognised within some NATO nations, who have barred the inclusion of internet sources in their assessments to mitigate some of the starker consequences of the internet era.

Whilst there are linguistic experts within the intelligence community, their work has traditionally been confined to the translation of oral testimony or of documents written in the appropriate third language.[58] But the predominant mode of western intelligence communities is to focus on English-language sources or to (mostly) machine translate foreign language sources into English. Given the workload pressures within the intelligence community, it is easy to see that questions of resourcing and scale are a considerable element of how and why there are these established preferences for English-language sources or translations into the English language. Intelligence Officers and analysts are simply too busy to place a considered emphasis on an all source mix that is geographically and culturally pluralistic. This situation has been attributed, in part, to the education system, in part to recruitment practices, and in part to the constraints placed by security and vetting officers. A form of caution or conservatism on the part of vetting officers is both explicable and partially understandable, particularly in the context of the potential dangers involved in allowing – for example – jihadist sympathisers into the intelligence community, with all that might entail.

One route around these potential security vulnerabilities would be to widen the participation of external contractors across the intelligence community – thus widening the community – and to employ forms of organisational offshoring and stovepiping, which would help to facilitate a larger pool of foreign language specialists into the concentric periphery of the IC, without unduly jeopardising security, whilst adding materials, and important nuance to these contextual materials.

The dominance of the English language and sources written in English is not only restricted to the analytical community but also dominates the academic community, and other expert pools as well. There is a small and thriving literature on the perils of anglo- and euro-centricity in the development of academic disciplines, which has – in turn – been translated into the initiative and movement to 'decolonise the curriculum'.[59] So, academic experts will – with very few exceptions – arrive with a partial fragment of the available academic materials on a subject, constrained by language, in addition to the usual constraints around disciplinary homogeneity. The information scientist Eugene Garfield was one of the first scholars to note how academic inquiry fragmented across disciplines, particular journals and geographical spaces. In doing so, he pioneered early concepts of the journal impact factors that most journals and scholars pay attention to.[60] The translation of citation analysis, impact factors and multidisciplinarity into an intelligence assessment environment is problematic due to the time and complexity this issue represents, but the end result is that an external academic expert presenting to, or advising a group of intelligence analysts will very rarely have incorporated academic research from Chinese, Russian or Iranian sources, to name but three of the west's principle adversaries, nor indeed citations to French or German language sources, where they have not been provided in a translated form at the source.

Given that cultural blindness has been linked to negative outcomes in the Vietnam war, the global war on terror, and in the Iraqi and Afghan theatres of operation, the failure to diversify sourcing and expertise seems an error for the intelligence community and for those academics seeking to garner impact from their research, whilst we should acknowledge that the professional incentive structures for academics do not lend themselves to multidisciplinary or multi-lingual work.[61] There are certainly prevailing internal university and external funder narratives promoting interdisciplinarity but the number of quality academic journals who are capable of processing or willing to public multidisciplinary work are few and far between, posing the researcher a choice between intellectual ambition and career expediency, which is underpinned by the marketisation of higher education.[62]

For the less sensitive areas of government, interaction with the UK's external expert community (across higher education, think-tank and third sectors) has been widely encouraged, and schemes put in place to facilitate it. There have been successive moves in central government to encourage civil servants not only to seek outside expert views but to have the implementation of policies tested by expert outsiders. In 2013, the UK Government established a network of seven independent centres to inform government decision-making through the provision of independently assessed evidence. The 'What Works Network' covers a range of policy areas, including: crime, health care, social care and education. Amongst others, the *London School of Economics* acts as a host for the *What Works Centre* dedicated to looking at local economic growth.[63] In 2015, the *What Works initiative* expanded further in its outreach to academia by establishing a *Cross-Government Trial Advice Panel*, funded by the Economic and Social Research Council (ESRC). The panel, comprising twenty-five academics, was established to educate civil servants in the use of experimental and quasi-experimental research methods.[64] By 2015, a considerable infrastructure had been put in place by the Cabinet Office to encourage civil servants to seek external expertise, including academia, to inform a wide range of policymaking areas under the *Open Policy Making* initiative, using the 'latest analytical techniques, and taking an agile, iterative approach to implementation'.[65] Whilst these initiatives are steps in the right direction, they lack the pervasive added value that an Open-Source Intelligence Agency would have, where contributions would not require officials to establish a commission of inquiry, but would enable experts to engage in providing verifiable data and assessments that can be utilised by government departments and intelligence organisations to support their activities.

Conclusion

Intelligence agencies of the Five Eyes group, but particularly of the UK and US, are systematically looking to engage with a wider pool of external experts drawn from private industry, public bodies, third sector organisations and universities. This engagement is uneven across the communities but more so in the UK where there are considerable organisational and philosophical barriers to it. Engagement with profit-seeking organisations has been impacted by the push factors of equipment sales and the pull factors of seemingly elegant solutions, rather than pursuing purely strategic decisions.

There is an intellectual case for refining and reforming existing engagements to improve the way they function and to enhance the value they add to each side. This incremental approach ranges from embedding more external experts into the intelligence community, through to moving towards experts as human sources. This article has argued that there is a far stronger intellectual case for a more radical change to how we understand the role of external expertise in intelligence, and how intelligence agencies seek, process and disseminate intelligence products, what the Rand Corporation described as 'third-generation OSINT', where the focus is in on refining dissemination.[66] This paradigm shift would move external experts from offering challenge to the agencies to being part of their intelligence collection and analysis effort, across a wider pool of subjects and within holistic analytical frameworks.

There are many synergies and benefits for national security agencies and the academic communities that work on these subjects from pursuing closer engagement through what I have described here as an iterative reform. The notion of embedding academics in a way that would be reminiscent of the American revolving door arrangements has its attractions in terms of providing added value to the government but it overshadowed by the practical and procedural challenges to it. The UK's National Crime Agency has tried to tackle this problem through their Special Officer programme which recruits niche capabilities from outside of the agency, and whilst this is said to include a number of academics it will be subject to large overheads of vetting and management costs. In 2017 the Cabinet Office opened a portal where academics could lodge the details of their research expertise and their contact details, but it was poorly advertised, and the professional associations – the *Political Studies Association* and *British International Studies Association* – also advertise opportunities for engagement, including those in Parliament. The absence of scale, as well as coherency, creates transaction costs for officials trying to engage with academics, provides for a largely informal system that depends on an officials professional network of contacts. From the academic perspective, this informality places a reliance upon securing external funding for engagements, and the goodwill of local university managers to help manage teaching and administrative schedules.

COVID-19 and the economic and social challenges from it, as one set of examples amongst many, provide the rationale for a new or expanded role for intelligence agencies in providing decision support to government, with a greater emphasis on holistic analytical models and multidisciplinary and multilingual open-source information gathering. There are open-source agencies and units on both sides of the Atlantic, but they have been placed within an intelligence architecture that privileges narrow quasi-military concerns around lethality, and which are geared to supporting the executive, rather than the whole of government and the legislature. Neither of these architectures support multidisciplinary and multilingual open-source discovery nor the translation of open-source discovery into decision support for all levels of government, and elected representatives.

The paradigm-shifting reform would be the creation of a national Open-Source Intelligence Agency in which the key knowledge-producing groups are represented, and in which there is a standing staff to manage the relationship between the Agency and government customers. The Agency's staff would also be tasked with disseminating the collected and analysed products to appropriate departmental customers. Such an agency would benefit from the inclusion of universities as organisations which are experienced in managing and disseminating cutting edge knowledge products. Universities would provide an ideal clearing house for open-source intelligence requirements, which could be taken up by students through declared intelligence assignments or dissertations. Similarly, a broad-base Open-Source Intelligence Agency could serve as revolving door for moving cognitively diversified talent into the covert intelligence community, something that is a priority for the community currently.[67] Viewed from a parochial British position, such an agency would have the soft-power potential akin to the BBC Monitoring Service to project British soft-power through the reliability of its information, making a contribution to diplomacy, development and trade. Within the US system, a greater emphasis on providing decision support is the necessary shift to for OSINT to begin to deliver on the promise it has been well known to have since the turn of the century.

The observations I conducted for this research suggest that the ideal-type relationship between external experts and practitioners is one premised on iterative and ongoing relations. Such relationships are substantially more valuable than the production of a context piece or a discreet piece of work that is framed around providing open-source challenge. Within the existing model of engagement, such ongoing relations are made problematic by requirements around security vetting, counterintelligence, managing multiple line managers and few career incentives to engage with the intelligence community. The 'sandbox' methodologies of engineering departments and the defence industries where a cleared senior academic manages a group of uncleared junior academics doing discreet or small tasks for which they do not know or understand the whole project they are working for have provided one means by which to manage this interaction within the existing model. An overhauled Open-Source Intelligence Agency model would remove much of the need to actively manage security risks, as the research and sourcing would remain open and counter-intelligence would be centred on avoiding undue foreign interference. There is understandable institutional inertia, which in turn leads to instinctive governmental preference to slowly evolve and iterate the relationship between external experts and their respective intelligence communities. While this remains the case, though, the considerable contributions that external experts could make on government efforts to mitigate the 'wicked problems' our countries face will be obscured.

Notes

1. EUCOM, "The United States European Command".
2. Eldridge et al, "Fusing Algorithms," 392.
3. Hulnick described OSINT as peculiarly effective as a tool for early warning: Hulnick, "The Dilemma of OSINT," 232.
4. The over-reading of the new-ness of globalisation is effectively rebutted by Justin Rosenberg. Rosenberg, "Globalisation Theory," 450-82. Marret is credited with coining the term 'glocal' in relation to Al-Qaeda: Marret, "Al-Qaeda," 543.
5. Barber, *Jihad vs McWorld*.
6. Mahbubani, *Has China Won?*
7. Davies and Gustafson, "Complexity, Uncertainty," 1–20.

8. Whilst Steven Stollemyre discusses automated forms of crowdsourcing for intelligence, my argument here could be seen to align to Stolleymyre's broad argument. "Solleymyre, HUMINT, OSINT or Something New?," 580.
9. Peter Gill makes a persuasive case for the role of intelligence during and after the pandemic: Gill, "Intelligence Oversight," 15.
10. UK Parliament, "COVID-19".
11. Ibid.
12. UK Government Office for Science, *Blackett Review*. As far back as 2004 Stevyn Gibson, an MoD official had called for enhanced OSINT to support military planning, in the light of the Hutton Report: Gibson, "Open Source Intelligence," 11.
13. Daily Telegraph, "Pandemic Unit Scrapped".
14. ESRC Impact Accelerator Account – University of Leicester.
15. Davies, "Intelligence Culture and Intelligence Failure," 519–20.
16. UKRI, COVID-19.
17. Clarke and Newman, "Brexit and the Paradoxes," 101–16.
18. Nunan and Stanier et al, "Eliciting Human Intelligence," 1-2.
19. See Manget's excellent survey of this subject: Manget, F, "Law Enforcement Intelligence," 189–211.
20. Wells & Gibson, "OSINT from a UK Perspective," 84–96; Carter & Carter, "Law enforcement intelligence," 139.
21. Dymydiuk, "RUBICON and revelation"; Dobson, "Operation Rubicon"; Walsh & Miller, "Rethinking Five Eyes Security"; Johnson et al, "Implications of the Snowden Leaks," 793–810.
22. In an interesting article, Craig Dudley describes this approach as "information centric intelligence," whilst he classifies the existing systems as 'analysis centric' intelligence. See: Dudley, "Information-Centric Intelligence," 762.
23. Adam, "Simulations," 316–8.
24. Gill, "Intelligence Oversight," 10–1.
25. Betsch, Wieler "Monitoring Behavioural Insights," 1255–65.
26. Jin et al, "Predicting Bank Failure," 2811–9; Hellmich, "Creating the Ideology," 112.
27. Clarke and Newman, "The Paradoxes of Brexit," 101–16.
28. Samtani et al, "Cybersecurity as an industry".
29. Steele, *On Intelligence*, 111–26.
30. Sims, "What is intelligence?" 5.
31. UK Cabinet Office, "Intelligence Assessment Academy," 2019.
32. Dover & Goodman, "The Public Policy Role," 342–51; Dover, Goodman and White, "Two Worlds, One Common Pursuit," 461–77.
33. Glees' fine history of the Stasi also initially underplayed the extent to which their officers were keen to overstate their successes, and he was not alone in this, including Markus Wolf's own account of his time at the Stasi. He is right, though, to point out that his papers did see several Stasi agents uncovered in the UK. See: Glees, *Stasi*, 62–3; Miller, *Narratives of Guilt*, 3–5; Wolf & McElvoy, *Spymaster*, pp365.
34. Herman, *Intelligence Power*, 13.
35. Nunan and Stanier et al, "Eliciting Human Intelligence," 1-2.
36. Miller, OSINT: An Oxymoron? 714.
37. The consequences when such an arrangement goes wrong are made clear by Nielson, "Whistleblowers," 660–89.
38. For a contemporary discussion of this area see: Scott, "Contemporary Security Vetting," 2020, 54–70.
39. Zegart and Morrell, "Spies, Lies and Algorithms," 83–96.
40. Gill, "Intelligence Oversight," 6–7.
41. Dymydiuk, "Rubicon and Revelation"; Miller, "OSINT: An Oxymoron?" 712.
42. Gibson, "OSINT," 11.
43. Gentry, "The All Source Mix," 649–50.
44. Lentzos et al, "Health Intelligence," 465–76.
45. As told by Gordon Corera in his book on the subject. Corera, *Shopping for Bombs*.
46. Jervis, *Why Intelligence Fails*, 15–34.
47. Aldrich et al, "Operation Rubicon".
48. The Times, "Professor Rosemary Hollis: Obituary".
49. These voices included notable area studies experts like Rosemary Hollis, George Joffé, Gareth Stansfield, Charles Glass, Toby Dodge and Eric Herring, who published widely in the academic and quality media on this subject, who provided evidence to Parliamentarians and who – in the case of Hollis – was able to brief officials directly. The Iraq Inquiry; Joffe, "Iraq Environment"; Dodge, "Causes and Consequences".
50. Parker, "Cummings' Job Ad".
51. One notable attempt to do this can be found in: Cudworth & Hobden, *Post-Human International Relations*.
52. Private conversation with former CIA Officer, January 2020.
53. Steele, "Open Source Intelligence," 144–7.
54. Kamali, S, "Informants".

55. Graham et al, “Internet Geographies,” 58.
56. McCarthy, “NSA”.
57. Galloway, “Blink and They’re Gone,” 969.
58. Arthur Hulnick noted this nearly 20 years ago, and it remains a considerable challenge. Hulnick, “The downside of OSINT,” 570–2.
59. Harvey & Russell-Mundine, “Decolonising the Curriculum,” 789.
60. Garfield, “Citation Analysis,” 471–9.
61. The strongest work of this type was written by Patrick Porter, see: Porter, *Military Orientalism*.
62. Bendixen and Jacobsen, “Marketisation,” 20.
63. UK Government, “What works networks,” 2015
64. UK Cabinet Office, “Cross Government Advice Panel,” 2015.
65. UK Government, “Open Government,” 2015.
66. Williams and Blum, *Defining 2nd Generation OSINT*, 40.
67. UK Parliament, *ISC Report on Diversity*, 65; and popularised by Matthew Syed: Syed, *Rebel Ideas*, 3–37.

Disclosure statement

No potential conflict of interest was reported by the author.

Notes on contributor

Dr Robert Dover is Associate Professor of Intelligence and International Security at the University of Leicester. He is the Convenor of the UK Political Studies Association’s Specialist Security and Intelligence Studies Group, and a previous winner of the Political Studies Association’s Wilfrid Harrison Prize for the Best Article in Political Studies. He has written more than 60 papers on the governmental use of intelligence, the impact of intelligence and surveillance upon social relations, horizon scanning, and crisis communications.

ORCID

Robert Dover http://orcid.org/0000-0002-2780-9729

Bibliography

Adam, D. “Special Report: The Simulations Driving the World’s Response to COVID-19.” *Nature* 580, no. 7803 (2020): 316–318. doi:10.1038/d41586-020-01003-6.

Aldrich, R., P. Müller, D. Ridd, and E. Schmidt-Eenboom. “Operation Rubicon: Sixty Years of German-American Success in Signals Intelligence.” *Intelligence and National Security* 35, no. 5 (2020): 603–607. doi:10.1080/02684527.2020.1774849.

Andrew, C. *The Defence of the Realm: The Authorised History of MI5*. London: Penguin, 2010.

Barber, B. *Jihad Vs McWorld*. New York: Times Books, 1995.

Bendixen, C., and J. C. Jacobsen. “Nullifying Quality: The Marketisation of Higher Education.” *Quality in Higher Education* 23, no. 1 (2017): 20–34. doi:10.1080/13538322.2017.1294406.

Betsch, C., L. Wieler, and K. Habersaat. “Monitoring Behavioural Insights Related to COVID-19.” *The Lancet* 395, no. 10232 (2020): 1255–1265. doi:10.1016/S0140-6736(20)30729-7.

Butler. *Review of Intelligence on Weapons of Mass Destruction*. London: HMSO, 2004.

Carter, J. G., and D. L. Carter. “Law Enforcement Intelligence: Implications for Self-radicalized Terrorism.” *Police Practice and Research* 13, no. 2 (2012): 138–154. doi:10.1080/15614263.2011.596685.

Chilcot, J. *The Iraq Inquiry*. London: HMSO, 2016.

Clarke, J., and J. Newman. “People in This Country Have Had Enough of Experts’: Brexit and the Paradoxes of Populism.” *Critical Policy Studies* 11, no. 1 (2017): 101–116. doi:10.1080/19460171.2017.1282376.

Cudworth, E., and S. Hobden. *Posthuman International Relations: Complexity, Ecologism and Global Politics*. London: Zed Books, 2011.

Davies, P. “Intelligence Culture and Intelligence Failure in Britain and the United States.” *Cambridge Review of International Affairs* 17, no. 3 (2004): 495–520. doi:10.1080/0955757042000298188.

Davies, P., and K. Gustafson. “Complexity, Uncertainty and a Military Intelligence Doctrine for the 21st Century.” *Political Studies Association Conference* (2015): 1–20.

Department of Defense, Defense Technical Information Centre. *Joint Publication 2-0, Joint Intelligence*. Createspace: Washington, DC, 2013.

Dobson, M. "Operation Rubicon: Germany as an Intelligence 'Great Power'?" *Intelligence and National Security* 35, no. 5 (2020): 608–622. doi:10.1080/02684527.2020.1774852.

Dodge, T. *What Were the Causes and Consequences of Iraq's Descent into Violence after the Initial Invasion?* London: The Iraq Inquiry, 2009. https://webarchive.nationalarchives.gov.uk/20120215203302/http://www.iraqinquiry.org.uk/articles.aspx.

Dover, R., and M. Goodman. *Learning Lessons from the Secret Past*. Washington: Georgetown University Press, 2011.

Dover, R., and M. Goodman. "The Public Policy Role of Intelligence Scholars." In *The Routledge International Handbook of Universities, Security and Intelligence Studies*, edited by L. Gearon, 342–351. Abingdon: Routledge, 2019.

Dover, R., M. Goodman, and M. White. "Chapter 25: Two Worlds, One Common Pursuit: Why Greater Engagement with the Academic Community Could Benefit the UK's National Security." In *The Palgrave Handbook of Security, Risk and Intelligence*, edited by R. Dover, H. Dylan, and M. Goodman, 461–477. London: Palgrave, 2017.

Dudley, C. "Information-Centric Intelligence: The Struggle in Defining National Security Issues." *International Journal of Intelligence and CounterIntelligence* 31, no. 4 (2018): 758–768. doi:10.1080/08850607.2018.1488503.

Dymydiuk, J. "RUBICON and Revelation: The Curious Robustness of the 'Secret' CIA-BND Operation with Crypto AG." *Intelligence and National Security* 35, no. 5 (2020): 641–658. doi:10.1080/02684527.2020.1774853.

Eldridge, C., C. Hobbs, and M. Moran. "Fusing Algorithms and Analysts: Open-source Intelligence in the Age of 'Big Data." *Intelligence and National Security* 33, no. 3 (2018): 391–406. doi:10.1080/02684527.2017.1406677.

EUCOM. 2020. "Welcome to the United States European Command." Accessed July 3 2020. https://www.eucom.mil/

Galloway, C. "Blink and They're Gone: PR and the Battle for Attention." *Public Relations Review* 43, no. 5 (2017): 969–977. doi:10.1016/j.pubrev.2017.06.010.

Gentry, J. "The "Professionalization" of Intelligence Analysis: A Skeptical Perspective." *International Journal of Intelligence and CounterIntelligence* 29, no. 4 (2016): 643–676. doi:10.1080/08850607.2016.1177393.

Gibson, S. "Open Source Intelligence." *The RUSI Journal* 149, no. 1 (2004): 16–22. doi:10.1080/03071840408522977.

Gibson, S. "Exploring the Role and Value of Open Source Intelligence." In *Open Source Intelligence in the Twenty-First Century New Approaches and Opportunities*, edited by C. Hobbs, M. Moran, and D. Salisbury, 9–23. Basingstoke: Palgrave, 2018.

Gill, P. "Of Intelligence Oversight and the Challenge of Surveillance Corporatism." *Intelligence and National Security* (2020): 1–20. doi:10.1080/02684527.2020.1783875.

Glees, A. "The Stasi's UK Operations: Subversion and Espionage', 1973–1989." *The Journal of Intelligence History* 7, no. 1 (2007): 61–82. doi:10.1080/16161262.2007.10555139.

Goodman, M. 2015. *Writing the Official History of the Joint Intelligence Committee*. Partnership for Conflict, Crime and Security Research. Accessed November 7 2016. www.paccsresearch.org.uk/blog/writing-the-official-history-of-the-joint-intelligence-committee/

Goodman, M. *The Official History of the Joint Intelligence Committee: 1*. Abingdon: Routledge, 2015.

Goodman, M., and D. Omand. "What Analysts Need to Understand: The Kings Intelligence Studies Programme." *Studies in Intelligence* 52/4 (2008): 57–65.(December 2008).

Graham, M., S. Ojanperä, and M. Dittus. "Internet Geographies." *Society and the Internet: How Networks of Information and Communication are Changing Our Lives* edited by Dutton, W & Graham, M, 58 (2019): 58-79. Oxford University Press: Oxford.

Harvey, A., and G. Russell-Mundine. "Decolonising the Curriculum: Using Graduate Qualities to Embed Indigenous Knowledges at the Academic Cultural Interface." *Teaching in Higher Education* 24, no. 6 (2019): 789–808. doi:10.1080/13562517.2018.1508131.

Hellmich, C. "Creating the Ideology of Al Qaeda: From Hypocrites to Salafi-Jihadists." *Studies in Conflict & Terrorism* 31, no. 2 (2008): 111–124. doi:10.1080/10576100701812852.

Herman, M. *Intelligence Power in Peace and War*. Cambridge: Cambridge University Press, 1996.

Heuer, R., and R. Pherson. *Structured Analytic Techniques for Intelligence Analysis*. New York: CQ Press, 2010.

Hulnick, A. "The Downside of Open Source Intelligence." *International Journal of Intelligence and CounterIntelligence* 15, no. 4 (2002): 565–579. doi:10.1080/08850600290101767.

Hulnick, A. "The Dilemma of Open Sources Intelligence: Is OSINT Really Intelligence?" In *The Oxford Handbook of National Security Intelligence*, edited by L. Johnson, 229–241. Oxford: Oxford University Press, 2010.

Jervis, R. *Why Intelligence Fails: Lessons from the Iranian Revolution and the Iraq War*. New York: Cornell University Press, 2010.

Jin, J., K. Kanagaretnam, and G. Lobo. "Ability of Accounting and Audit Quality Variables to Predict Bank Failure during the Financial Crisis." *Journal of Banking & Finance* 35/11 (2011): 2811–2819. doi:10.1016/j.jbankfin.2011.03.005.

Joffe, G. *Iraq and Its Environment before March 2003*. London: The Iraq Inquiry, 2009. https://webarchive.nationalarchives.gov.uk/20120215210701/http://www.iraqinquiry.org.uk/articles/environment.aspx.

Johnson, L. K., R. J. Aldrich, C. Moran, D. Barrett, G. Hastedt, R. Jervis, W. Krieger, et al. "An INS Special Forum: Implications of the Snowden Leaks." *Intelligence and National Security* 29, no. 6 (2014): 793–810. doi:10.1080/02684527.2014.946242.

Johnston, R. *Analytic Culture in the US Intelligence Community: An Ethnographic Study*. Langley: CIA, 2005.

Kamali, S. “Informants, Provocateurs, and Entrapment: Examining the Histories of the FBI’s PATCON and the NYPD’s Muslim Surveillance Program.” *Surveillance & Society* 15, no. 1 (2017): 68–78. doi:10.24908/ss.v15i1.5254.

Kent, S. *Strategic Intelligence for American World Policy*. Princeton: Princeton University Press, 1949.

Lancaster University. 2015. National Centre for Research and evidence on Security Threats. Accessed November 5 2015. www.lancaster.ac.uk/security-lancaster/news-and-events/news/2015/national-centre-for-research-and-evidence-on-security-threats/

Lentzos, F., M. S. Goodman, and J. M. Wilson. “Health Security Intelligence: Engaging across Disciplines and Sectors.” *Intelligence and National Security* 35, no. 4 (2020): 465–476. doi:10.1080/02684527.2020.1750166.

Mahbubani, K. *Has China Won?: The Chinese Challenge to American Primacy*. New York: Ingram Publishers, 2020.

Manget, F. “Intelligence and Law Enforcement.” In *The Oxford Handbook of National Security Intelligence*, edited by L. Johnson, 189–211. Oxford: Oxford University Press, 2010.

Marret, J. L. “Al-Qaeda in Islamic Maghreb: A “Glocal” Organization.” *Studies in Conflict & Terrorism* 31, no. 6 (2008): 541–552. doi:10.1080/10576100802111824.

McCarthy, K. *After Blowing $100m to Snoop on Americans’ Phone Call Logs for Four Years, What Did the NSA Get? Just One Lead*. Accessed June 24 2020. San Francisco: The Register, 2020. https://www.theregister.com/2020/02/26/nsa_calllogging_program/last

Miller, B. *Narratives of Guilt and Compliance in Unified Germany: Stasi Informers and Their Impact on Society*. Abingdon: Routledge, 1999.

Miller, B. H. “Open Source Intelligence (OSINT): An Oxymoron?” *International Journal of Intelligence and CounterIntelligence* 31, no. 4 (2018): 702–719. doi:10.1080/08850607.2018.1492826.

National Crime Agency. *Special Officer Scheme*. Accessed June 1 2020. www.nationalcrimeagency.gov.uk/careers/specials

Nielsen, R. P. “Reformed National Security Internal Whistleblowing Systems and External Whistleblowing as Countervailing Ethics Methods.” *Administration & Society* 52, no. 5 (2020): 660–689. doi:10.1177/0095399718760583.

Nunan, J., Stanier, I., Milne, R., Shawyer, A., & Walsh, D. (2020). Eliciting human intelligence: Police source handlers’ perceptions and experiences of rapport during CHIS interactions. *Psychiatry, Psychology and Law*, 1-27.

Parker, G. *Dominic Cummings Job Ad Opens Number 10 to ‘Wild Cards’ and ‘Assorted Weirdos*. London: Financial Times, 2020. January 2.

Porter, P. *Military Orientalism: Eastern War Through Western Eyes*. London: Hurst, 2009.

Rosenberg, J. “Globalization Theory: A Post Mortem.” *International Politics* 42 (2005): 2–74. doi:10.1057/palgrave.ip.8800098.

Rosenberg, J. “International Relations — The ‘Higher Bullshit’: A Reply to the Globalization Theory Debate.” *International Politics* 44 (2007): 450–482. doi:10.1057/palgrave.ip.8800200.

Samtani, S., M. Abate, V. Benjamin, and W. Li. “Cybersecurity as an Industry: A Cyber Threat Intelligence Perspective.” In *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, edited by T. Holt and A. Bossler, 135–154. 2020. Palgrave: Basingstoke.

Scott, P. “The Contemporary Security Vetting Landscape.” *Intelligence and National Security* 35, no. 1 (2020): 54–71. doi:10.1080/02684527.2019.1665688.

Sims, J. “What Is Intelligence? Information for Decision Makers.” In *U.S. Intelligence at the Crossroads: Agenda for Reform*, edited by R. Godson, E. May, and G. Schmitt, pp. 3-17. Washington DC: Brasseys, 1995.

Steele, R. D. *On Intelligence: Spies and Secrecy in an Open World*. Fairfax VA: AFCEA International Press, 2000.

Steele, R. “Open Source Intelligence (Operational).” In *Handbook of Intelligence Studies*, edited by L. Johnson (Chapter 10), 129–147. NY: Routledge, 2008.

Stern, N. *Research Excellence Framework Review: Building on Success and Learning from Experience*. London: HMSO, 2016.

Stollemyre, S. “HUMINT, OSINT, or Something New? Defining Crowdsourced Intelligence.” *International Journal of Intelligence and CounterIntelligence* 28, no. 3 (2015): 578–589. doi:10.1080/08850607.2015.992760.

Syed, M. *Rebel Ideas: The Power of Diverse Thinking*. London: John Murray, 2019.

The Daily Telegraph. 2020 14 June. ‘Boris Johnson ‘Scrapped Cabinet Pandemic Committee Six Months before Coronavirus Hit UK’, *The Daily Telegraph*: London.

The Times. 2020 June 22. ”Professor Rosemary Hollis Obituary”, *The Times*. London. https://www.thetimes.co.uk/article/professor-rosemary-hollis-obituary-5sb528gb2

UK Cabinet Office. 2015. *The Cross-Government Trial Advice Panel*. London: HMSO. Accessed November 6 2015. www.gov.uk/government/uploads/system/uploads/attachment_data/file/451336/the_Cross-Government_Trial_Advice_Panel.pdf

UK Cabinet Office. 2019. “Head of the Intelligence Assessment Academy.” Accessed June 24 2020. https://cabinetofficejobs.tal.net/vx/mobile-0/appcentre-1/brand-2/candidate/so/pm/1/pl/16/opp/3977-3977-Head-of-the-Intelligence-Assessment-Academy/en-GB

UK Government. August 2015. *The What Works Network*. London: HMSO. Accessed November 6 2015. www.gov.uk/guidance/what-works-network

UK Government. 2015. “*Open Government Blog*.” Accessed November 6 2015. https://openpolicy.blog.gov.uk/tools-and-techniques/

UK Government. 2016. *Horizon Scanning Programme Team*. Accessed November 7 2016. www.gov.uk/government/groups/horizon-scanning-programme-team

UK Government Office for Science. *Blackett Review of High Impact Low Probability Risks*. Ref: BIS/12/519. London: HMSO, 2012.

UK Parliament. *Intelligence and Security Committee: Diversity and Inclusion in the UK Intelligence Community - 2018 Report*. London: HMSO, 2018.

UK Parliament. 2020. "UK Parliamentary Office for Science and Technology." Accessed June 24 2020. https://post.parliament.uk/category/analysis/covid-19/

UK Research and Innovation. "Get Funding for Ideas that Address COVID-19." Accessed June 24 2020. https://www.ukri.org/funding/funding-opportunities/ukri-open-call-for-research-and-innovation-ideas-to-address-covid-19/

Walsh, P., and S. Miller. "Rethinking 'Five Eyes' Security Intelligence Collection Policies and Practice Post Snowden." *Intelligence and National Security* 31, no. 3 (2016): 345–368. doi:10.1080/02684527.2014.998436.

Wells, D., and H. Gibson. "OSINT from a UK Perspective: Considerations from the Law Enforcement and Military Domains." In *Proceedings Estonian Academy of Security Sciences, 16: From Research to Security Union* edited by Maasing, H, 84–113. Estonian Academy of Security Sciences, 2017.

Williams, H., and I. Blum. *Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise*. California: RAND Corporation, 2018.

Wolf, M., and A. McElvoy. *Man without a Face: The Autobiography of Communism's Greatest Spymaster*, 365. New York: Times Books, 1997.

Zegart, A., and M. Morrell. "Spies, Lies, and Algorithms: Why U.S. Intelligence Agencies Must Adapt or Fail." *Foreign Affairs* May/June 2019 (2019): 83–96.